UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,958	01/23/2004	Takatoshi Ono	82478-4800	7878

21611 7590 06/04/2007

SNELL & WILMER LLP (OC)
600 ANTON BOULEVARD
SUITE 1400
COSTA MESA, CA 92626

EXAMINER	
JUNG, DAVID YIUK	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/763,958	ONO ET AL.	
	Examiner	Art Unit	
	David Y. Jung	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) 1-14 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) 1-14 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 3/06;3/04.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-14 are presented.

CLAIM REJECTIONS

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaminaga (cited by Applicant, Kaminaga European Patent Application No. EP 1 237 322) and Biehl (cited by Applicant, Biehl et al., "Differential Fault Attacks on Elliptic Curve Cryptosystems", Advances in Cryptology, 20th Annual International Cryptology Conference, Aug. 20-24, 2000. Proceedings, Lecture Notes in Computer Science; Vol. 1880 Berlin, Springer, DE 20 August 2000, pp. 131-146) and Antipa (cited by Applicant, Antipa et al., "Validation of elliptic curve public keys", Public Key Cryptography-PKC 2003 6th International Workshop on Practice and Theory in Public Key Cryptography, 6 January 2003, pp. 211-223.

Regarding claim 1, Kaminaga teaches "An elliptic curve exponentiation apparatus that computes an elliptic curve exponentiation for an elliptic curve

E:y2=x3+aXx+b defined over a residue field F with a prime p being a modulus, comprising: an information obtaining unit operable to obtain a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p; a first storage unit operable to store therein a coefficient a that is an x term of the elliptic curve E; a computation unit operable to compute an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point k'Q; (pages 10-11, paragraphs 0056-0071, figures 11-13, e.g., the case of characteristic of field being 2 as described at paragraph 0057)."

These passages of Kaminaga are not explicit regarding "a judgment unit operable to judge whether the obtained exponentiation-result-point k*Q is on the elliptic curve E" in the sense of the claim.

Antipa teaches "a judgment unit operable to judge whether the obtained exponentiation-result-point k*Q is on the elliptic curve E; and an output unit operable to output the obtained exponentiation-result-point k'Q, when a judgment result of the judging unit is affirmative (section 5: Preventing Invalid Curve Attacks, i.e., making sure that the point is on the elliptic curve) for the motivation of greater security (abstract) when handling elliptic curves (pages 215-216).

These passages of Kaminaga and Antipa are not explicit regarding "an output unit operable to output the obtained exponentiation-result-point k'Q, when a judgment result of the judging unit is affirmative."

Biehl teaches "an output unit operable to output the obtained exponentiation-result-point k'Q, when a judgment result of the judging unit is affirmative (section 6:

Countermeasures i.e., tamper-proof device to check the output point or any point which serves as the basis for the computation of some output values)" for the motivation of greater security when handling elliptic curves (section 2: elliptic curves).

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the teachings of Kaminaga, Antipa, and Biehl for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Claims 1, 10, 12, 13 are the independent claims.

Claims 10 (information security analog to claim 1), claim 12 (method analog), claim 13 (computer program analog) are analogs to claim 1. For the reasons noted in the rejection of claim 1, these claims are unpatentable.

Claims 2-9 recite various calculations in accordance with the formula noted in claim 1. These calculations are well known in the art for the motivation of computing when actuating elliptic curves. See, in particular, cited sections 3 and 4 of Antipa and cited section 2 of Biehl.

Claim 11: such plaintext, etc. are well known applications of elliptic curve handling for the motivation of cryptography.

Claim 14: computer readable medium is well known and standard for recording data.

Conclusion

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background.

Points of Contact

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(571) 273-8300, (for formal communications intended for entry)

Or:

(571) 273-3836 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (571) 272-3836 or Kambiz Zand whose telephone number is (272) 272-3811.

David Jung

Patent Examiner

5/30/07